Industrial Engineering and Innovation Management (2025)
Clausius Scientific Press, Canada

DOI: 10.23977/ieim.2025.080214
ISSN 2522-6924 Vol. 8 Num. 2

Data Security in Industrial IoT: Challenges and Emerging Solutions

Fei Lu[1,2,a], Haojing Huang[1,b], Zhiming Cai[3,c,*], Jian Chen[3,d]

[1] *School of Engineering and Technology, Guangdong Polytechnic Institute, Guangzhou, China*
[2] *Faculty of Data Science, City University of Macau, Macau, China*
[3] *Faculty of Digital Science and Technology, Macau Millennium College, Macau, China*
[a] *flu@gdrtvu.edu.cn,* [b]*huanghj@gdrtvu.edu.cn,* [c]*zmcai@mmc.edu.mo,* [d]*kech05@me.com*
**Corresponding author*

Keywords: Industrial Internet of Things, Data Security, Edge Computing, Lightweight Distributed Ledger

Abstract: The implementation of Industrial Internet of Things (IIoT) is significantly constrained by the emergence of Data security. This paper examines the primary data security issues and protection mechanisms associated with IIoT, providing a comprehensive analysis of how security protection systems evolve across the stages of data collection, transmission, storage, and processing. The focus is directed towards advancements in edge computing and lightweight distributed ledger technologies, which significantly enhance data security. The paper begins with a review of the evolution and development of IIoT, highlighting the challenges that current technologies present in effectively addressing data privacy, integrity, real-time performance, and scalability. Following this, the analysis focuses on the efficacy of edge computing to mitigate data exposure while simultaneously improving computational efficiency. Additionally, the study examines the benefits of lightweight distributed ledger technologies for resource-constrained environments, highlighting their role in ensuring data immutability and enhancing data transparency. The paper concludes by analyzing potential trends in IIoT data security technologies, such as post-quantum cryptography, AI-driven security protections, and zero-trust architectures, and by offering perspectives on the future of technological advancements.

1. Introduction

The Industrial Internet of Things (IIoT)[1] represents a convergence of industrial machinery, computational systems, and human intelligence through ubiquitous sensing and advanced machine learning, changing the way traditional operations work to build intelligent, efficient, and sustainable ecosystems. Ultimately, IIoT aims to achieve unprecedented performance through precision automation, increased productivity, and optimized resource utilization across various industrial sectors. The McKinsey Global Institute anticipates that the IoT economy will generate between USD 3.9 trillion and USD 11.1 trillion in annual value by 2025, spanning various sectors, including retail, urban development, and manufacturing. Additionally, device deployments are expected to exceed 754 billion units[2]. Further analysis suggests that the number of IoT-connected devices in

the World could reach nearly 40 billion within the next decade (2030)[3]. In the face of such dramatic growth, the security, real-time responsiveness, reliability, and scalability of IIoT systems are pillars that must be addressed as priorities, and doing so will be key to ensuring the resiliency and stability of industrial infrastructure while enabling organizations to adopt IIoT technologies at scale and sustainably, across multiple applications.

The security technologies related to the IIoT—such as lightweight encryption, differential privacy, fog computing-based security architectures, multi-layer deep defense, unidirectional network devices, and relevant security standards—have significantly enhanced the security of data transmission, storage, and access. The IIoT market is expected to reach approximately $844.82 billion by 2030[4], but the increasing scale of systems poses considerable challenges regarding device diversity, network reliability, and data privacy protection. According to the Zscaler ThreatLabz 2024 Mobile, IoT, & OT Threat Report, industries engaged in IIoT are key targets for malware attacks. The manufacturing sector accounts for 36% of all attacks, and the transportation sector also accounts for 14%. Therefore, investigating IIoT data security is of considerable scientific and commercial importance. Adequate security measures are essential to ensure the reliable operation of IIoT and to achieve its full commercial potential. The security protection requirements for IIoT data include identity authentication, data protection, secure data transmission, anomaly detection, real-time computation, and data encryption. These components are crucial strategies to safeguard IIoT security. A comprehensive security approach can provide enterprises with greater efficiency and safety in industrial production and operations.

The paper identifies key challenges related to data security arising from the evolution and challenges of IIoT, and then presents advancements in edge computing and lightweight distributed ledger technologies as solutions to enhance data security protection. It also aims to discuss the future technological trends.

2. Overview of Industrial Internet of Things Development

Fueled by advancements in sensor capabilities, the rapid development of wireless communication technologies, and the widespread adoption of cloud computing, the IIoT has evolved beyond mere device interconnection to create large-scale, intelligent, and highly efficient integrated systems. The system architecture retains the core features of traditional IoT frameworks while increasingly addressing the requirements for real-time responsiveness, reliability, and security. This shift marks the emergence of Industry 4.0[5], the era of smart manufacturing. Compared to traditional methods, the use of the IIoT enables enterprises to more effectively monitor various stages of production processes in real-time, predict equipment failures, and optimize production flows. This also helps achieve greater efficiency improvements and reduced costs. Furthermore, IIoT provides enterprises with an even greater opportunity for innovation in their business models, such as remote maintenance and customized production. Furthermore, the recent emergence of new technologies such as 5G, edge computing[6], and artificial intelligence has further expanded and deepened the potential applications of the IIoT, increasing its compatibility and usability in industrial scenarios.

The industrial Internet of Things (IIoT), as a critical agent of industrial digital transformation, has exerted a strong influence on global industrial policy. In 2019, Germany published the document "Germany Industry Strategy 2030: Guidelines for a German and European Industrial Policy"[7] to bolster Germany's global competitiveness through innovation, industrial restructuring, and international cooperation, while promoting digitalisation and sustainability. Likewise, in an effort to address disconnected data initiatives, as seen in the above example, but on a European scale, the European Union published "A European Strategy for Data" in 2020[8]. This proposed a

1‘European data space’, encouraging data sharing and reuse to enhance value-adding processes across industries and in industrial data use cases, such as the IoT and artificial intelligence. In the long term, this will foster innovation in the EU's digital economy and enhance its global competitiveness. Unlike previous approaches, Industry 5.0[9,10], introduced in 2021, utilizes intelligent and adaptive applications to analyze and predict human and machine behavior, enabling zero-touch operations. In doing so, it exemplifies how European and American countries place greater emphasis on IIoT and digital transformation through strategic planning.

China unveiled the Industrial Internet Innovation and Development Action Plan (2021–2023) [11] in 2021 to accelerate the nationwide establishment of an industrial internet identification and resolution system, promoting intelligent transformation across a broad range of industries. In parallel, the United States introduced the National Cybersecurity Strategy [12] in 2023, outlining targeted measures to address IIoT security challenges. These national initiatives underscore the strategic importance attributed to IIoT security and development, with the U.S. strategy specifically incorporating directives focused on IIoT protection.

The advancement of national strategies highlights the growing significance attributed to the development of the IIoT. Nevertheless, the large-scale interconnection of data in practical deployments has introduced new security risks. IIoT has been widely used in critical areas such as manufacturing, energy, logistics, supply chain, and agriculture, where many sensors are used to collect data to monitor and manage industrial equipment and production processes in real time in order to sustain stable, efficient system performance. Concurrently, emerging paradigms such as Cloud Manufacturing (CMfg) [13], the Internet of Vehicles (IoV) [14], and the Internet of Drones (IoD) [15] are providing an enabling capacity for real-time data analytics and intelligent decision-making. Large-scale interconnection and cross-domain data sharing impose greater security challenges. Similarly, the increased interaction and sharing of multi-source data in IIoT networks have generated threats, including privacy violations and data tampering. Due to this, securing data security is a significant issue and an area worthy of discussion, which is the primary focus of this paper.

3. Research Progress on Data Security Issues in IIoT

The IIoT has steadily progressed towards more interconnected, automated, and intelligent systems that improve production efficiency and productivity while eliminating unnecessary costs. The growing IIoT ecosystem, characterized by extended sensory data collection, open data streams, and lightweight architecture, places additional pressure on vulnerabilities amid numerous risks and security threats that were initially discussed from multiple perspectives[16]. Numerous threats exist across a combination of endpoints by data acquisition at the perception layer, data transmission at the network layer, and data processing at the application layer.

3.1. Data Collection Security Issues

At the perception layer, the data collection phase is primarily susceptible to security threats, including device vulnerabilities, physical damage, data eavesdropping, data tampering, and identity spoofing. Arguably, unauthorized access and bypassing identity authentication can lead to malicious data insertion or device tampering, whereas plaintext data transmission poses a heightened risk of interception and decryption. The vulnerability of perception devices to physical damage and malicious code attacks posed a significant threat to the integrity of data collection from the source. Hence, attention to these issues thoroughly in data collection at the perception layer is important to preserving data integrity and privacy.

Strengthening identity authentication mechanisms at the perception layer is a necessary step in

combating the aforementioned risks. Implementing identity authentication in data collection at the industrial IoT perception layer is a viable and effective method. The authentication mechanism provides a feasible assurance for communication security among devices, between users, and services. The industry and academia have begun proposing several authentication solutions in recent years, including blockchain-based solutions, lightweight protocols, anonymizing techniques, and biometrics. It has been demonstrated to be an effective method for enhancing data security. Table 1 summarizes some of the typical identity authentication schemes and their characteristics studied in academia, including blockchain-based solutions, lightweight protocols, anonymizing techniques, and biometrics, to help provide a reference to combating the associated issues.

Table 1 Research on Identity Authentication in Industrial Internet of Things (IIoT).

Category	Solution Description	Key Features
Blockchain Technology Application [17]	Uses blockchain technology for device identity authentication, data sharing, traceability, and certificate revocation	Decentralized, data immutability, enhanced security, and privacy protection.
Lightweight Authentication Protocol [18]	Reduces computational and communication overhead, suitable for resource-constrained IIoT devices	Lightweight design, low resource requirements, suitable for resource-constrained environments.
Privacy Protection and Anonymity Technology [19]	Achieves user and device privacy protection and anonymous authentication, using group signatures, proxy re-encryption, and other techniques	Privacy protection, anonymous authentication, and data security.
Three-Factor Authentication [20,21]	Utilizes three authentication factors (biometrics, passwords, and credentials)	Triple authentication, edge computing integration, dynamic identity revocation, and session key negotiation.
Unobservable fingerprinting signature [22]	Uses unobservable fingerprinting signatures combined with function data analysis methods to provide a concealed and efficient authentication mechanism	Anti-detection, fingerprint features, supports MQTT 5.0, and functions for data analysis.

Despite recent progress, current research on data security authentication in the IIoT continues to be constrained by several significant limitations. First, compared with small-scale implementations, the scalability and processing speed of blockchain technology in large-scale IIoT systems remain particularly challenging. Second, although lightweight protocols are advantageous for resource-constrained devices, the equilibrium between lightweight design and comprehensive security remains elusive. Third, enhancing authentication efficiency and usability alongside protecting privacy remains a technical challenge that necessitates further advancement. Some researchers have proposed introducing lightweight distributed ledger technology into identity authentication to leverage its decentralization, privacy protection, and immutability features, thereby enhancing security in resource-constrained environments. However, this direction remains underexplored, and no mature solution has been established.

3.2. Data Transmission Security Issues

In IIoT, wireless transmission serves as the primary method for data communication, while its openness exposes communication data to numerous security threats[23]. Common attacks include eavesdropping (passively listening to communication content), where attackers obtain sensitive data through wireless sniffing, jeopardizing privacy and business secrets[24]; data tampering, which involves unauthorized interception and malicious modification of transmitted data that results in distorted measurements or forged control commands; man-in-the-middle attacks, where attackers intervene between communication parties and impersonate legitimate nodes to carry out eavesdropping and tampering; and signal interference/blockage (interference attacks), wherein electromagnetic noise is generated at the physical layer or frequency bands are blocked. These disruptions prevent everyday communication between devices and cause network and service disruptions, as well as service failures[25]. These attacks compromise data confidentiality and

integrity, and in severe cases, can cause automatic control systems at industrial sites to malfunction or cease production, resulting in safety and economic losses. Hence, end-to-end encryption, strict identity authentication mechanisms, and anti-interference technologies must be implemented to safeguard data security during transmission. For example, establishing a zero-trust authentication and encryption channel in wireless links can prevent eavesdropping and tampering. Interference attacks can be mitigated through frequency hopping and dynamic scheduling, thereby enhancing network resilience. Table 2 compares the main security risks and typical protective mechanisms of several commonly used communication technologies in IIoT.

Table 2 Overview of Major Security Threats and Protective Mechanisms for Typical Communication Technologies in Industrial Internet of Things (IIoT).

Communication Technology	Major Security Risks	Protective Mechanisms and Countermeasures
5G Cellular Networks	Complex features, such as network slicing and virtualization, may introduce new security vulnerabilities; the physical layer is also susceptible to interference.	Utilize 5G-AKA authentication and end-to-end encryption to ensure secure access; isolate data flows for different applications using network slicing strategies; and introduce anti-interference technologies, such as frequency hopping and adaptive scheduling, to enhance tolerance to malicious interference.
Wi-Fi Wireless Local Area Networks [26]	Wireless channels are vulnerable to eavesdropping, message forgery, and interference attacks, with risks of unauthorized access.	Deploy WPA3 encryption protocol and 802.1X identity authentication; segment and isolate industrial Wi-Fi networks, configuring intrusion detection systems to detect and block suspicious man-in-the-middle attacks and signal interference sources promptly.
Low-Power Wide Area Networks	Attackers may manipulate data using replay or bit-flipping techniques; long-distance wireless transmission is also susceptible to eavesdropping and interference.	Utilize lightweight end-to-end encryption and integrity checks, and introduce device fingerprint authentication and physical-layer intrusion detection to identify unauthorized nodes and signal anomalies.
Edge Networks [27]	Internal attackers may eavesdrop on local communications or inject malicious data into the broadcast domain, threatening the system's collaborative security.	Strictly control access permissions to edge networks and deploy distributed intrusion detection/prevention systems to identify abnormal traffic. Combine blockchain and machine learning technologies to establish trust and collaborative defense mechanisms among edge devices, enabling intelligent protection against spoofed nodes and data injection attacks.

The security threats experienced during the data transmission stage are quite damaging, requiring immediate attention to deploy comprehensive safeguarding mechanisms that enable the steady operation of industrial systems. While securing the transmission links is critical, the security threats in the subsequent data storage and processing activities also need to be managed and will be discussed in the next section.

3.3. Data Storage and Processing Security Issues

In the IIoT realm, data possesses characteristics of large-scale generation, heterogeneously stored, and processed in real-time. This poses the issue of data security as a core problem facing organizations and governments globally. Research has found that security issues at the storage and processing stages have the potential to disrupt operational productivity and threaten the stability of global supply chains.

Due to its critical economic importance, the manufacturing industry has become a key target for IIoT attacks. A compromise to an industrial control system can lead to an immediate disruption to production lines and the supply chain, thereby creating a severe operational disruption. IBM X-Force's "Cost of a Data Breach Report 2024" indicates that the global average cost of a data breach in 2024 is $4.88 million, representing a 10% increase from 2023 and marking the most pronounced escalation since the COVID-19 pandemic. An Accenture survey [28] indicates that approximately 55%

of industrial storage systems are internet-connected, with about 40% lacking essential access controls. Furthermore, 72% of organizations report an increase in network risks in 2024 compared to previous years. This security gap makes attacks, such as ransomware and data theft, particularly impactful. The International Data Corporation (IDC) forecasts that by 2025, the global data volume in the industrial sector will reach 73.1 zettabytes (ZB). Approximately 70% of this data will require long-term storage or frequent access, thereby increasing exposure to potential cyberattacks.

A significant portion of industrial enterprises continues to rely on outdated storage technologies. According to Gartner, more than 35% of industrial storage devices have been in use for over six years, which poses challenges in supporting modern encryption algorithms and dynamic authentication mechanisms. This "technical debt" creates vulnerabilities, making these devices prime targets for cyberattacks. With the increasing adoption of edge computing devices in IIoT systems, their security measures fall short of addressing 75% of the data processing tasks they manage. The "2024 Benchmark Report on IoT Security" by Palo Alto Networks reveals that the average cost of a data breach in the U.S. in 2023 was $9.5 million. However, current technologies are inadequate in securing IoT device data, with 51% of respondents acknowledging that their existing solutions are insufficient to protect IoT devices within the network. A notable example occurred in 2024, when a car manufacturer suffered a data breach that exposed the location data of 800,000 electric vehicles online. This incident underscores significant weaknesses in vehicle data storage security [29].

IIoT systems often require the integration of data from diverse platforms and devices, including sensor networks, industrial control systems (ICS), and third-party applications. According to Deloitte[30], 46% of companies view data ownership and security as the leading challenge to IIoT deployment, highlighting data management and protection as more significant barriers than previously anticipated.

To counteract the risk of data breaches, enterprises must urgently enhance the security of their storage devices, adopt modern protection mechanisms, and introduce AI-driven automated security defenses. In response to these demands, the upcoming section examines the potential of an IIoT data security framework. This framework combines edge computing with distributed ledger technology to provide more secure storage and processing.

4. Edge Computing to Address Data Exposure Issues

Edge computing plays a pivotal role in data transmission in the IIoT. By moving data processing closer to the data source at edge nodes, sensitive data can be processed locally without requiring it to be sent back to the cloud. The procedure will reduce data exposure during long-distance transmission and enhance security. To reduce network latency, lower cloud bandwidth costs, and enhance data processing speed in critical applications, real-time responses provide an effective solution. Edge computing is widely utilized in manufacturing, energy management, and transportation systems, enabling rapid data analysis and supporting informed decision-making. This method is particularly effective for fields with stringent real-time response requirements, such as manufacturing, energy management, and transportation systems.

In recent years, significant progress has been made in edge computing technology. As shown in Table 3, the typical edge computing frameworks and their focal points over the past five years are summarized, covering aspects such as data processing algorithms, edge intelligence, vehicular computing, and resource scheduling. These research outcomes primarily focus on integrating deep learning, artificial intelligence, 5G networks, and innovations in federated learning and blockchain technology. Future research will emphasize addressing data privacy and security issues in edge computing, as well as optimizing resource management, scheduling, and computational efficiency

in heterogeneous network environments.

Table 3 Analysis of Edge Computing Research Frameworks Over the Past Five Years.

Technology Framework	Problem Solved	Unresolved Issues
Fusion of Deep Learning and Edge Computing [31]	Integration of edge computing and deep learning.	Issues with data privacy and security, as well as energy consumption and resource constraints of edge devices, have not been fully addressed.
Edge Intelligence [32]	Deployment of AI models to the edge, achieving the "last mile" of AI applications.	The difficulty in handling the heterogeneity of edge devices necessitates the optimization of resource management.
Vehicular Edge Computing [33]	Distributed task offloading and on-demand resource allocation.	Integration of demand forecasting into collaborative task computing and resource management.
Federated Learning and Blockchain [34]	Data synchronization framework for integrating federated learning, edge computing, and blockchain.	Bottlenecks in data synchronization and model updates in federated learning environments.
Neuro-Fuzzy Systems and Blockchain [35]	New security multi-access edge computing VANET (Vehicular Ad-hoc Network) based on neuro-fuzzy systems and blockchain.	Adaptability and scalability issues in dynamic network environments of VANET.
Smart Healthcare Systems [36]	Edge computing in smart healthcare systems.	Privacy Protection and Compliance Issues for Medical Data.
Distributed Signal Processing and Edge Learning [37]	Edge learning and distributed signal processing in 5G networks: semantic communication, edge computing, and wireless sensing.	Wireless signal processing and resource allocation in 5G networks still need optimization.
Artificial Intelligence and Machine Learning [38]	AI edge computing framework	Optimization and deployment of machine learning models in edge computing.

As shown in Table 3, recent edge computing research has focused on areas such as integration with artificial intelligence, network collaboration, and security protection. On one hand, applications of deep learning and federated learning at the edge have enhanced data processing intelligence. Still, challenges like privacy and energy consumption need to be addressed. On the other hand, incorporating technologies such as blockchain and encryption into edge architectures, as seen in federated learning and blockchain integration, as well as neuro-fuzzy blockchain frameworks (Table 2), suggests that researchers are exploring ways to enhance the security of edge computing. However, these studies primarily focus on performance optimization. There is still room for further development in security topics such as data encryption, access control, and intrusion detection at the edge layer.

Edge computing in the IIoT enhances data processing efficiency, real-time decision-making, and data privacy by enabling local data processing. This reduces reliance on cloud storage, conserves bandwidth, and mitigates the risk of data breaches from central node attacks. Recent research has proposed key algorithm models to optimize edge computing. These include distributed data processing, edge intelligence, resource allocation, security algorithms, and federated learning. These models aim to improve real-time analysis, decision-making, resource utilization, and security. The combination of these models boosts edge computing's capabilities to safely analyze industrial data, allocate resources efficiently, and transfer and update the sharing of models. Thus, we can see applications of edge computing in smart transportation, robotics and industrial automation, and healthcare. Still, challenges may arise due to the finite processing and storage capabilities of edge nodes. Future research should consider addressing edge computing security through the use of application-based controls, local encryption, trusted execution environments, and intrusion detection. This is especially important for industries such as manufacturing, energy management, and transportation, which require prompt and accurate real-time responses.

5. Lightweight Distributed Ledger Technology to Address Data Security Issues

IIoT nodes face computational constraints, hindering the deployment of complex security systems. Zscaler reports that over 87% of cyber threats are concealed within encrypted traffic[39]. However, attackers can exploit this encryption to mask malicious activities, posing significant challenges to traditional security monitoring. This highlights the need for new security mechanisms. Lightweight distributed ledger technologies, such as IOTA Tangle and Hyperledger Iroha, offer promising solutions. Their decentralized and immutable properties provide efficient data protection in resource-constrained environments, improving security, transparency, and efficiency. These technologies are especially suited for industrial environments. They enable secure data storage and sharing without relying on central servers, thus mitigating single points of failure. Additionally, distributed ledgers ensure the immutability of data records, thereby enhancing data credibility for regulatory compliance and supply chain transparency. In real-time monitoring and remote operations, they also facilitate faster data exchange, enabling quicker and more informed decision-making. The integration of lightweight distributed ledger technology into IIoT enhances data security, reliability, and collaboration efficiency. Table 4 summarizes the progress of the research on commonly used lightweight distributed ledger technologies.

Table 4 Major Lightweight Distributed Ledger Technologies and Their Features.

Technology Name	Function Description	Key Features	Open Source
IOTA Tangle [40]	Distributed ledger based on DAG (no blockchain), specifically designed for IoT.	Eliminates the traditional blockchain structure, improves its lightweight nature, and increases transaction speed.	Yes
Nano [41]	Uses Block Lattice structure, each account has its own blockchain.	Employs an account chain structure, where each account maintains its blockchain.	Yes
Hyperledger Iroha[42]	Distributed ledger designed for mobile applications and IoT devices.	Simplified architecture, fast transaction processing.	Yes
Corda[43]	A distributed ledger is primarily used for financial services, with a focus on enhancing transaction efficiency and privacy.	Suitable for enterprise applications, it provides privacy protection.	Yes
Quorum[44]	Enterprise-level blockchain platform based on Ethereum, modified to support high-speed transactions and privacy protection.	Suitable for enterprise applications, it enhances transaction speed and privacy.	Yes
Holochain [45]	Uses a proxy architecture without a global consensus, where each node maintains its chain and engages in peer-to-peer interaction.	Allows devices to maintain their chain and engage in peer-to-peer interaction without relying on global consensus.	Yes

6. Future Development Directions

Over the next 55 years, emerging technologies will profoundly influence data security and protection mechanisms for the IIoT. They will also influence security threats and the development of new regulatory frameworks. As industries accelerate the deployment of IIoT, there is a need to adopt advanced, forward-looking, and scalable security measures to ensure the resilience, efficiency, and security of IIoT infrastructure. The following analysis examines key trends and strategies in IIoT data protection for the years ahead.

6.1. The Widespread Adoption of Post-Quantum Cryptography (PQC) and Quantum-Resistant Networks

Numerous IIoT systems are anticipated to integrate post-quantum cryptography (PQC)[46-48] to mitigate the risks posed by quantum computing. Over the forthcoming five to ten years, it is expected that quantum-resistant encryption protocols will achieve widespread adoption within IIoT infrastructure. This will ensure that IIoT devices, communication channels, and cloud services are adequately fortified against threats originating from quantum computing. IIoT systems may utilize quantum key distribution (QKD) or various quantum-safe communication protocols to achieve this transformation. These safeguards help ensure that data transferred, even in the most remote and most crucial industrial spaces, is quantum-secure. For example, QKD is designed to establish secure data channels between sensors and centralized systems, as well as to facilitate quantum-safe communication. Quantum safeguards ensure that the transfer of sensitive industrial data is resilient, dependable, secure, and regulated, even in the presence of an adversary with quantum capabilities.

By permitting the use of modular encryption architectures, III stakeholders can smoothly transition into new algorithms as quantum-resistant technologies advance, an improvement over previous approaches. Such proactive measures mitigate the risk of quantum decryption more efficiently than traditional reactive tactics, preserving the integrity and confidentiality of the data over time.

6.2. Mechanisms for Autonomous Security Operations with Artificial Intelligence and Machine Learning

The continued incorporation of artificial intelligence (AI) into IIoT systems[49-51] will thrust autonomous security operations, powered by machine learning (ML) and next-generation AI models, into a primary role in the overall security of the IIoT. AI-empowered security systems will support real-time threat detection with autonomous decision-making and self-healing capabilities, thereby maintaining the integrity and security of IIoT networks. AI-driven threat hunting, an exciting development in this space, enables machine learning algorithms to continuously scan IIoT devices and network behavior, uncovering anomalies and pre-emptively predicting potential threats, thereby securing IIoT from security incidents before they occur. The predictive AI model represents a breakthrough in protecting against emerging cybersecurity risks, including zero-day vulnerabilities, ransomware, and insider threats, achieving a level of truly proactive protection.

By enabling IIoT to autonomously isolate infected devices, block malicious data flows, and initiate recovery protocols, AI-driven incident response will also facilitate the efficient and expedited management of security incidents, eliminating the need for human intervention. The adoption of these autonomous security technologies allows industrial operators to maintain business continuity, thereby reducing downtime and mitigating the impact of cyberattacks. IIoT manufacturers are urged to directly integrate AI capabilities into edge devices to realize this objective, thereby enabling real-time decision-making at the data source. These devices will employ edge computing to process and analyze substantial volumes of data, thereby enhancing response speed and minimizing delays in security operations.

6.3. The Practical Application of Lightweight Distributed Ledger Technology

Blockchain technology is presently employed in IIoT scenarios, including supply chain management, asset tracking, and industrial automation, to guarantee data integrity and authenticity. Nonetheless, traditional blockchain solutions introduce new data security and privacy challenges due to the constrained computational abilities of perception layer devices. This situation highlights

the pressing necessity for lightweight security solutions. Lightweight distributed ledger technology [52-54] is expected to gain widespread acceptance within the IIoT ecosystem, ensuring transparency, timeliness, and security in data exchange.

Distributed ledger technology is likely to play a crucial role in ensuring that data can be both immutable and traceable within IIoT networks, particularly in situations where data authenticity is a critical requirement. For instance, within smart manufacturing, blockchain technology can be utilized to create certification mechanisms for data generated by machines and sensors, thereby mitigating data tampering and ensuring accuracy and reliability in the production process. Additionally, it is likely that smart contracts will be prevalent within IIoT for the automatic execution of secure transactions between machines, sensors, and users. These self-executing contracts will ultimately help ensure that all actors within a supply chain or industrial network operate under the agreed-upon terms and conditions, thereby minimizing disputes and leading to improved efficiencies over time.

To achieve this, more and more IIoT manufacturers will allocate budget for integrating blockchain into existing industrial networks. Integration platforms are already in development that will allow existing industrial networks to integrate blockchain protocols while also providing scalability and high performance.

6.4. Zero Trust Architecture Becomes the Standard

The security philosophy of Zero Trust Architecture (ZTA) is characterized by a lack of trust in any device or user within both internal and external networks[55-57]. Unlike conventional approaches, the Zero Trust principle is expected to become a foundational element of IIoT network security in the coming years. It mandates rigorous authentication and authorization processes for each device and engineer account, even within internal networks, prior to granting access to critical devices such as Programmable Logic Controllers (PLCs). Functionally, this requirement significantly mitigates internal threats. The escalation of network attack complexity and the proliferation of devices suggest that conventional perimeter defense models may not meet the demands. Zero Trust networks are a vital security model for protecting IIoT systems against internal and external threats, as they provide ongoing verification of identity, authorization, and validation at every level of the IIoT ecosystem, compared to other mechanisms. The principle can be extended to all connections and interactions between devices, systems, and users or applications, resulting in the continuous enforcement of security policy in real-time.

When deploying Zero Trust-based Identity and Access Management (IAM) tools across IIoT environments, Zero Trust assurance provides certainty that every connected device, user, or service must go through strict identity verification prior to accessing sensitive data or executing critical operations. This will substantially increase the difficulty for an attacker in overcoming any security, access, or data protection measures. Finally, deploying the model through integration of multi-factor authentication (MFA), micro-segmentation, and policy evaluation in IIoT systems provides real-time monitoring and responses to security threats across the entire IIoT environment.

6.5. Proactive Security Risk Management and Event Prediction

In the context of cybersecurity, leveraging large-scale pre-trained models represents a significant paradigm shift, as security defenses transition from a reactive to a proactive approach. Artificial intelligence and data analysis enable the cybersecurity industry to predict and mitigate risks before industrial systems become targets of attack. Future AI security technologies will leverage historical attack data and assess environmental factors, discrepancies, and anomalies within systems to anticipate potential security incidents. This will allow the organization to formulate and initiate

proactive risk mitigation strategies. Once a risk is identified, the technology will autonomously adjust security policy and reroute data through secure pathways, while advancing patches or initiating recovery procedures on affected or compromised devices and networks to prevent an attacker from abusing and exploiting the vulnerability.

As part of this transformation, IIoT network resilience frameworks will be developed and integrated to support the system in recovering quickly and minimizing operational disruptions, even in the event of a security breach. Resilient architecture, real-time monitoring, and rapid response capabilities will be crucial in mitigating the risk of network attacks and ensuring the long-term stability of IIoT infrastructure. Due to the heterogeneous nature of IIoT, data security will continue to integrate with technologies such as quantum resistance, AI-driven security, blockchain integration, Zero Trust architecture, and data privacy regulations. Achieving a forward-looking IIoT strategy architecture— including supply chain optimization, smart manufacturing, production optimization, and vehicle networking (as shown in Figure 1)—that combines these key technologies will ensure the success and resilience of IIoT systems in the next decade. By adopting advanced technologies and transforming their security architecture, industrial enterprises can protect their IIoT networks from future threats while unlocking new efficiencies, scalability, and innovative potential.

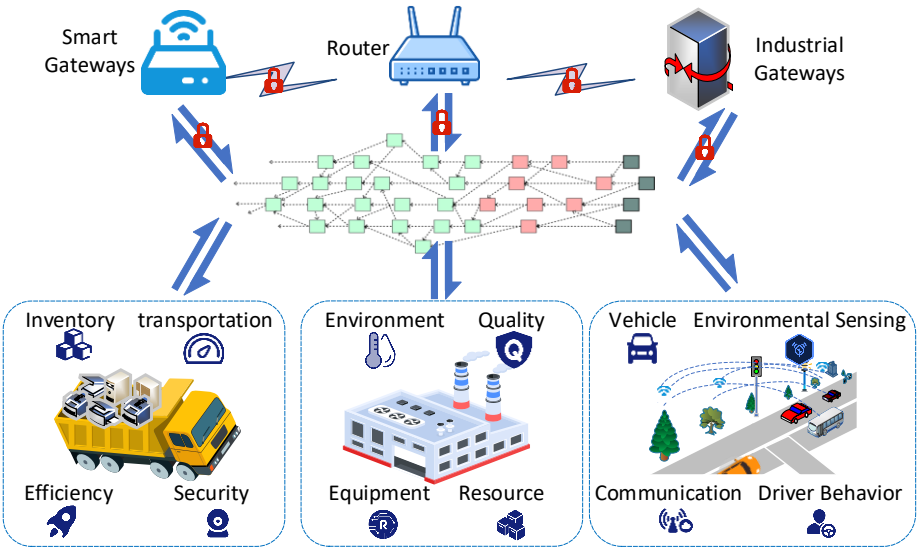

Figure 1 Edge Cluster Architecture Based on Distributed Ledger.

Figure 1 illustrates the prototype of the future IIoT security architecture, where edge computing clusters are integrated with distributed ledgers to implement security strategy convergence in scenarios such as supply chain optimization, smart manufacturing, and the Internet of Vehicles (IoV). This integration enables IIoT to manage and share data efficiently and securely. Compared to conventional approaches, the convergence of these technologies not only enhances the security and transparency of data but also improves the system's reliability and resistance to attacks, providing a stronger foundation for the future development of IIoT and advancing smart manufacturing and automation.

With the progressive integration of technologies like quantum resistance, artificial intelligence, blockchain, and Zero Trust, the scope of data security will continue to evolve over time. Industrial enterprises must proactively plan and adopt advanced security architectures to protect III from future threats. In addition, they should leverage these new technologies to achieve greater efficiency and unlock their full innovation potential. Combining edge computing and lightweight blockchain constitutes a practical pathway. This combination illustrates the substantial potential of cross-

domain technology integration in IIoT security. This approach not only enhances real-time data processing capabilities but also strengthens system security and trust, providing a robust foundation for the advancement of IIoT over the next decade.

Acknowledgements

The authors gratefully acknowledge support for this study from the Project of 2024 Guangdong Polytechnic Institute (Project No. 2024CGPY002, 2025KCJS011); Guangdong Philosophy and Social Sciences Planning Greater Bay Area Research Special Project "Research on the Mechanism of Cross regional Data Compliance Flow in the Guangdong Hong Kong Macao Greater Bay Area" (GD23SQGL03); Guangdong Provincial Science and Technology Plan Project "Research on Precise Policy Implementation Path for High tech Enterprises Based on Enterprise Exclusive Service Space: Taking Hengqin Guangdong Macao Deep Cooperation Zone as an Example" (No. 2024A101005002), and the talent project of the Open University of Guangdong, “Research on Key Technologies for Improving the Performance of Blockchain Application Platforms” (Project No. 2021F001).

References

[1] SISINNI E, SAIFULLAH A, HAN S, et al. Industrial internet of things: Challenges, opportunities, and directions [J]. IEEE transactions on industrial informatics, 2018, 14(11): 4724-4734.
[2] ULLAH I, ADHIKARI D, SU X, et al. Integration of data science with the intelligent IoT (IIoT): current challenges and future perspectives [J]. Digital Communications and Networks, 2024, 10(1): 1-19.
[3] MYROSHNYK Y. State of IoT Summer 2024 [Z]//MYROSHNYK Y. 2024
[4] 360IRESEARCH. Industrial Internet of Things Market by Component (Hardware, Services, Software), Connectivity (Satellite Connectivity, Wired Connectivity, Wireless Connectivity), End-User—Global Forecast 2025–2030 [Z]. 360iResearch / Global Information, Inc. 2024
[5] MUNIRATHINAM S. Chapter Six - Industry 4.0: Industrial Internet of Things (IIOT) [M]//RAJ P, EVANGELINE P. Advances in Computers. Elsevier. 2020: 129-164.
[6] LUO Q, HU S, LI C, et al. Resource Scheduling in Edge Computing: A Survey [J]. IEEE Communications Surveys & Tutorials, 2021, 23(4): 2131-2165.
[7] ENERGY F M F E A A. German Industrial Strategy 2030: Guidelines for a German and European Industrial Policy [R]. Berlin, 2019.
[8] COMMISSION E. A European Strategy for Data [R]. Brussels, 2020.
[9] IVANOV D. The Industry 5.0 framework: viability-based integration of the resilience, sustainability, and human-centricity perspectives [J]. International Journal of Production Research, 2023, 61(5): 1683-1695.
[10] COELHO P, BESSA C, LANDECK J, et al. Industry 5.0: The Arising of a Concept [J]. Procedia Computer Science, 2023, 217: 1137-1144.
[11] LIN H, JIANJUN Y, SHA W, et al. Construction and Implementation Path for Industrial Internet Standards System in China [J]. Strategic Study of Chinese Academy of Engineering, 2021, 23(2): 88-94.
[12] HOUSE T W. National Cybersecurity Strategy [Z]. The White House, Office of the National Cyber Director. 2023
[13] ABUHASEL K A, KHAN M A. A Secure Industrial Internet of Things (IIoT) Framework for Resource Management in Smart Manufacturing [J]. IEEE Access, 2020, 8(6): 117354-117364.
[14] ZHOU H, XU W, CHEN J, et al. Evolutionary V2X technologies toward the Internet of vehicles: Challenges and opportunities [J]. Proceedings of the IEEE, 2020, 108(2): 308-323.
[15] PU C, WALL A, CHOO K K R, et al. A Lightweight and Privacy-Preserving Mutual Authentication and Key Agreement Protocol for Internet of Drones Environment [J]. IEEE Internet of Things Journal, 2022, 9(12): 9918-9933.
[16] HUO R, ZENG S, WANG Z, et al. A Comprehensive Survey on Blockchain in Industrial Internet of Things: Motivations, Research Progresses, and Future Challenges [J]. IEEE Communications Surveys & Tutorials, 2022, 24(1): 88-122.
[17] YANG H, BAO B, LI C, et al. Blockchain-enabled tripartite anonymous identification trusted service provisioning in industrial IoT [J]. IEEE Internet of Things Journal, 2021, 9(3): 2419-2431.
[18] YIN D, GONG B. A Lightweight Certificateless Mutual Authentication Scheme Based on Signatures for IIoT [J]. IEEE Internet of Things Journal, 2024, 11(16): 26852-26865.
[19] CASTIGLIONE A, NAPPI M, RICCIARDI S. Trustworthy method for person identification in IIoT environments by

means of facial dynamics [J]. IEEE Transactions on Industrial Informatics, 2020, 17(2): 766-774.
[20] ZHANG Z, HUANG W, HUANG Y, et al. A Domain Isolated Tripartite Authenticated Key Agreement Protocol With Dynamic Revocation and Online Public Identity Updating for IIoT [J]. IEEE Internet of Things Journal, 2024, 11(9): 15616-15632.
[21] ZHU W, CHEN X, JIANG L. A secure and efficient authentication key agreement scheme for industrial internet of things based on edge computing [J]. Alexandria Engineering Journal, 2024, 101: 52-61.
[22] KOPROV P, FANG X, STARLY B. Machine identity authentication via unobservable fingerprinting signature: A functional data analysis approach for MQTT 5.0 protocol [J]. Journal of Manufacturing Systems, 2024, 76: 59-74.
[23] AHMED S F, SHAWON S S, BHUYIAN A, et al. Forensics and security issues in the Internet of Things [J]. Wireless Networks, 2025, 31(4): 3431-3466.
[24] HASAN M K, WEICHEN Z, SAFIE N, et al. A survey on key agreement and authentication protocol for internet of things application [J]. IEEE access, 2024, 12(4): 61642-61666.
[25] MICHAELIDES S, LENZ S, VOGT T, et al. Secure integration of 5G in industrial networks: State of the art, challenges and opportunities [J]. Future Generation Computer Systems, 2024: 107645.
[26] RUOTSALAINEN H, SHEN G, ZHANG J, et al. LoRaWAN Physical Layer-Based Attacks and Countermeasures, A Review [J]. Sensors, 2022, 22(9): Article NO. 3127.
[27] ALOTAIBI B. A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities [J]. Sensors, 2023, 23(17): Article NO. 7470.
[28] FORUM W E, ACCENTURE. Global Cybersecurity Outlook 2025 [Z]//FORUM W E. World Economic Forum. 2025
[29] ROTH E. Volkswagen leak exposed location data for 800,000 electric cars [Z]//ROTH E. 2024
[30] INSIGHTS D. From "hindsight" to "foresight" - releasing the value of the Internet of Things industrial field [Z]//INSIGHTS D. Deloitte. 2023
[31] WANG X, HAN Y, LEUNG V C M, et al. Convergence of Edge Computing and Deep Learning: A Comprehensive Survey [J]. IEEE Communications Surveys & Tutorials, 2020, 22(2): 869-904.
[32] ZHOU Z, CHEN X, LI E, et al. Edge Intelligence: Paving the Last Mile of Artificial Intelligence With Edge Computing [J]. Proceedings of the IEEE, 2019, 107(8): 1738-1762.
[33] LIU L, FENG J, MU X, et al. Asynchronous Deep Reinforcement Learning for Collaborative Task Computing and On-Demand Resource Allocation in Vehicular Edge Computing [J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(12): 15513-15526.
[34] NGUYEN D C, DING M, PHAM Q V, et al. Federated Learning Meets Blockchain in Edge Computing: Opportunities and Challenges [J]. IEEE Internet of Things Journal, 2021, 8(16): 12806-12825.
[35] M P, BOUROUIS S, AHMED A N, et al. A Novel Secured Multi-Access Edge Computing based VANET with Neuro fuzzy systems based Blockchain Framework [J]. Computer Communications, 2022, 192(8): 48-56.
[36] HARTMANN M, HASHMI U S, IMRAN A. Edge computing in smart health care systems: Review, challenges, and research directions [J]. Transactions on Emerging Telecommunications Technologies, 2022, 33(3): e3710.
[37] GUO J, CHEN H, SONG B, et al. Distributed Task-Oriented Communication Networks with Multimodal Semantic Relay and Edge Intelligence [J]. IEEE Communications Magazine, 2024, 62(6): 82-89.
[38] HUA H, LI Y, WANG T, et al. Edge Computing with Artificial Intelligence: A Machine Learning Perspective [J]. ACM Comput Surv, 2023, 55(9): Article NO. 184.
[39] ZSCALER. Zscaler Finds Over 87% of Cyberthreats Hide in Encrypted Traffic, Reinforcing the Need for Zero Trust [Z]. web; Zscaler. 2024
[40] GUO F, XIAO X, HECKER A, et al. A theoretical model characterizing tangle evolution in IOTA blockchain network [J]. IEEE Internet of Things Journal, 2022, 10(2): 1259-1273.
[41] ZHANG C, ZHAO M, LIANG J, et al. Nano: Cryptographic enforcement of readability and editability governance in blockchain databases [J]. IEEE Transactions on Dependable and Secure Computing, 2023, 21(4): 3439-3452.
[42] WOZNICA A, KEDZIORA M. Performance and scalability evaluation of a permissioned Blockchain based on the Hyperledger Fabric, Sawtooth and Iroha [J]. Computer Science and Information Systems, 2022, 19(2): 659-678.
[43] QURESHI M U, GRAUX D, ORLANDI F, et al. Auto-generation of blockchain-based distributed applications using ontologies [M]. Blockchain and Smart-Contract Technologies for Innovative Applications. Springer. 2024: 217-258.
[44] MAZZONI M, CORRADI A, DI NICOLA V. Performance evaluation of permissioned blockchains for financial applications: The ConsenSys Quorum case study [J]. Blockchain: Research and applications, 2022, 3(1): Article NO.100026.
[45] JNR B A, SYLVA W, WATAT J K, et al. A framework for standardization of distributed ledger technologies for interoperable data integration and alignment in sustainable smart cities [J]. Journal of the Knowledge Economy, 2024, 15(3): 12053-12096.
[46] HUANG Z, WANG H, CAO B, et al. A comprehensive side-channel leakage assessment of CRYSTALS-Kyber in

IIoT [J]. Internet of Things, 2024, 27: Article NO. 101331.
[47] XIONG J, SHEN L, LIU Y, et al. Enhancing IoT security in smart grids with quantum-resistant hybrid encryption [J]. Scientific Reports, 2025, 15(1): Article NO. 3 (2025).
[48] CASTIGLIONE A, ESPOSITO J G, LOIA V, et al. Integrating Post-Quantum Cryptography and Blockchain to Secure Low-Cost IoT Devices [J]. IEEE Transactions on Industrial Informatics, 2024, 21(2): 1-10.
[49] QUY V K, NGUYEN D C, VAN ANH D, et al. Federated learning for green and sustainable 6G IIoT applications [J]. Internet of Things, 2024, 25: Article NO. 101061.
[50] KARACAYıLMAZ G, ARTUNER H. A novel approach detection for IIoT attacks via artificial intelligence [J]. Cluster Computing, 2024, 27(6): 10467-10485.
[51] SHOUKAT S, GAO T, JAVEED D, et al. Trust my IDS: An explainable AI integrated deep learning-based transparent threat detection system for industrial networks [J]. Computers & Security, 2025, 149: Article NO. 104191.
[52] DING X, WANG J, ZHAO Y, et al. Lightweight batch authentication and key agreement scheme for IIoT gateways [J]. Journal of Systems Architecture, 2025: 103368.
[53] ZHUANG C, DAI Q, ZHANG Y. A secure and lightweight data management scheme based on redactable blockchain for Digital Copyright [J]. Computer Standards & Interfaces, 2025, 91(3): Article NO. 103875.
[54] MEHMOOD F, KHAN A A, WANG H, et al. BLPCA-ledger: A lightweight plenum consensus protocols for consortium blockchain based on the hyperledger indy [J]. Computer Standards & Interfaces, 2025, 91(3): Article NO. 103876.
[55] ZANASI C, RUSSO S, COLAJANNI M. Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures [J]. Ad Hoc Networks, 2024, 156(12): Article NO. 103414.
[56] SINGH A, DHANARAJ R K, SHARMA A K. Personalized device authentication scheme using Q-learning-based decision-making with the aid of transfer fuzzy learning for IIoT devices in zero trust network (PDA-QLTFL) [J]. Computers and Electrical Engineering, 2024, 118(3): Article NO. 109435.
[57] ALEISA M A. Blockchain-Enabled Zero Trust Architecture for Privacy-Preserving Cybersecurity in IoT Environments [J]. IEEE Access, 2025, 13(1): 18660 - 18676.